UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,452	03/01/2004	Hiroshi Furukawa	16869Y-108700US	3451

20350 7590 02/28/2008
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
02/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/791,452	**Applicant(s)** FURUKAWA ET AL.	
	Examiner ANDREW L. NALVEN	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/9/08*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-8,12,13,15-18,21 and 22* is/are pending in the application.

4a) Of the above claim(s) *12 and 13* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-8,15-18,21 and 22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *2/12/08*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-3, 5-9, 12-13, 15-18, and 21-22 are pending. Claims 12 and 13 are withdrawn from further consideration.

Response to Arguments

2. Applicant's arguments filed 1/9/2008 have been fully considered but they are not persuasive.

3. Applicant has argued on pages 9-11 that Chirashnya fails to teach a traffic measuring and judging unit which measures traffic of all communication packets received in the interface, and traffic of a communication packet judged not to be the packet with said format in said first filter, respectively and by using the both traffics, judges whether a communication failure is generated or not. Examiner respectfully disagrees. Chirashnya teaches a traffic measuring and judging unit which measures traffic of all communication packets received in the interface, and traffic of a communication packet judged not to be the packet with said format in said first filter, respectively (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected, paragraph 0073, paragraph 0074), and by using the both traffics, judges whether a communication failure is generated or not (Chirashnya, paragraph 0047, monitors look for packet corruption). Chirashnya teaches the above limitation by teaching the measurement of packets that

are in an incorrect format (Chirashnya, paragraph 0047, corrupted packets, paragraph 0065) and traffic of all communication packets (Chirashnya, paragraph 0047, statistics indicating abnormal functionality such as devices not responding). Thus, Chirashnya does teach measuring two types of packet traffic: corrupted packets to look for incorrectly formatted packets and all packets in order to determine abnormal functionality or devices no longer responding. Further, Chirashnya's system then determines whether to trigger a failure alarm using the collected statistics (Chirashnya, paragraphs 0059-0060).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. **Claims 1 and 9 are rejected under 35 U.S.C. 102(e)** as being anticipated by Chirashnya et al US PGPub 2002/0019870.

5. **With regards to claim 1,** Chirashnya teaches a storage subsystem which is connected to a host computer through a communication line (Chirashnya, paragraph 0047, node comprised of storage subsystem connected to network), comprising an

interface which is used for connecting to said communication line (Chirashnya, paragraph 0047, nodes interconnected by switches), wherein, said interface comprises a first filter which judges, on the occasion of having received communication packets from said communication line, whether there is a communication packet with a predetermined format for use in an access to said storage subsystem, among the communication packets (Chirashnya, paragraph 0047, monitors look for packet corruption); wherein said interface further comprises a traffic measuring and judging unit which measures traffic of all communication packets received in the interface, and traffic of a communication packet judged not to be the packet with said format in said first filter, respectively (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected, paragraph 0073, paragraph 0074), and by using the both traffics, judges whether a communication failure is generated or not (Chirashnya, paragraph 0047, monitors look for packet corruption), and a communication failure alerting unit which alerts a management server connected to said storage subsystem (Chirashnya, paragraph 0047, generates alarm, paragraph 0048, alarms are sent to primary node) and comprises a function of displaying information alerted, in case that it is judged that a communication failure is generated in said traffic measuring and judging unit (Chirashnya, paragraph 0069, receive alarms and generate recommendations, paragraph 0059, user interface).

6. **With regards to claim 9,** Chirashnya teaches a computer readable storage medium including a program for a computer mounted on a storage subsystem connected to a host computer through a communication line (Chirashnya, paragraph

0047, node comprised of storage subsystem connected to network), the program comprising: code for connecting to said communication line (Chirashnya, paragraph 0047, nodes interconnected by switches); code for judging, on the occasion of having received communication packets from said communication line through connecting to said communication line, whether there is a communication packet with a predetermined format for use in an access to said storage subsystem, among the communication packets (Chirashnya, paragraph 0047, monitors look for packet corruption); code for receiving the communication packet judged to be for said access in said judging, and judges whether it is a communication packet permitted to access to a storage area in said storage subsystem and transmitted from said host computer or not (Chirashnya, paragraph 0047, monitors look for packet corruption); code for measuring traffic of all communication packets received in connecting to said communication line, and traffic of a communication packet judged not to be the packet with said format in said first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected, paragraph 0073, paragraph 0074); and code for alerting a management server connected to said storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring said traffic of all communications packets received in connecting to said communication line (Chirashnya, paragraph 0069, receive alarms and generate recommendations, paragraph 0059, user interface).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 2-3, 5-7 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Chirashnya et al US PGPub 2002/0019870 in view of Yoshida et al US Patent No. 6,622,220.

8. **With regards to claim 2,** Chirashnya fails to teach said interface further comprises a second filter which receives the communication packet judged to be for said access in said first filter, and judges whether it is a communication packet permitted to access to a storage area in said storage subsystem and transmitted from said host computer or not. However, Yoshida teaches said interface further comprises a second filter which receives the communication packet judged to be for said access in said first filter, and judges whether it is a communication packet permitted to access to a storage area in said storage subsystem and transmitted from said host computer or not (Yoshida, column 4 lines 6-26, determines if permission to access network storage device should be granted). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Yoshida's method of determining

access rights with Chriashnya's network diagnostic system because it offers the advantage of improving the security of network storage devices by preventing impersonation attacks (Yoshida, column 2 lines 4-10 and column 6 lines 1-26).

9. **With regards to claim 3,** Chirashnya as modified teaches that wherein, in case that said host computer is permitted to access to said storage subsystem, said interface further comprises an access permission table having information which uniquely specifies the host computer (Yoshida, column 5 lines 1-20, client access permissions, column 6 lines 25-35, access control list), and information which specifies a storage area in said storage subsystem to which the host computer is permitted to access, and said second filter judges whether a communication packet judged to be for use in said access is transmitted from the host computer permitted to access or not, in accordance with information stored in said access permission table (Yoshida, column 5 lines 10-25, validates requests on a per packet basis in view of the client access permissions).

10. **With regards to claim 5,** Chirashnya teaches said traffic measuring and judging unit further measures traffic of a communication packet, and by using the traffic and said traffic of all communication packets, further judges whether a communication failure is generated or not (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected), but fails to teach the communication packet being one that is judged not to be the communication packet transmitted from said host computer which is permitted to access in said second filter. However, Yoshida teaches the communication packet being one that is judged not to be the communication packet transmitted from said host computer which is

permitted to access in said second filter (Yoshida, column 9 lines 55-67, table 1, if packet not permitted, trigger alarm). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Yoshida's method of determining access rights with Chriashnya's network diagnostic system because it offers the advantage of improving the security of network storage devices by preventing impersonation attacks (Yoshida, column 2 lines 4-10 and column 6 lines 1-26).

11. **With regards to claim 6,** Chirashnya as modified teaches said interface further comprises a traffic log recording unit which records, as a traffic log, communication information of a communication packet judged not to be the communication packet with said format in said first filter and a communication packet judged not to be the communication packet transmitted from said host computer permitted to access in the second filter (Yoshida, column 9 lines 55-67, table 1, log the denied storage request, Chirashnya, paragraphs 0047-0048, event collection of packet corruption).

12. **With regards to claim 7,** Chirashnya as modified teaches a management server connected to the storage subsystem according to claim 6 (Chirashnya, paragraph 0048, management functions in primary node), wherein, an improper communication source analyzing unit which refers to said traffic log, in case that it is alerted from a communication failure alerting unit of said storage subsystem that a communication failure is generated, and searches a source of said communication packet causes the communication failure (Yoshida, column 9 lines 55-67, table 1, log the denied storage request, Chirashnya, paragraph 0059, look for greater failure rate than expected from

stored statistics).

13. **Claims 8 and 15-18 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Chirashnya et al US PGPub 2002/0019870 and Yoshida et al US Patent No. 6,622,220, as applied to claim 7 above, and in further view of Gleichauf US Patent No. 7,137,145.

14. **With regards to claim 8,** Chirashnya as modified fails to teach a relay device control unit which controls, based on information of a source searched in said improper communication source analyzing unit, a relay device which relays communication to said storage subsystem disposed on said communication line so as to cut off communication from the source. However, Gleichauf teaches a relay device control unit which controls, based on information of a source searched in said improper communication source analyzing unit, a relay device which relays communication to said storage subsystem disposed on said communication line so as to cut off communication from the source (Gleichauf, column 8 lines 18-27, records numbers of attempts to break firewall, column 9 lines 1-30, pattern or data matching, column 13 lines 15-20, communication may be disabled). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Gleichauf's method of cutting off communications because it offers the advantage of allowing the isolation of an invective or attacking network element thus reducing the danger of loss of data or system integrity (Gleichauf, column 1 lines 40-55, column 2 lines 45-60).

15. **With regards to claim 15,** Chirashnya teaches a storage system in which a storage subsystem, a host computer, and a management server are connected by a communication line (Chirashnya, paragraph 0048, management functions in primary node, paragraph 0047, node comprised of storage subsystem connected to network), wherein, said storage subsystem comprises an interface which connects to said communication line, and said interface comprises, a first filter which judges, on the occasion of having received communication packets from said communication line, whether there is a communication packet with a predetermined format for use in an access to said storage subsystem, among the communication packets (Chirashnya, paragraph 0047, monitors look for packet corruption), a traffic measuring and judging unit which measures traffic of all communication packets received in the interface, and traffic of a communication packet judged not to be the packet with said format, respectively, and by using the both traffics, judges whether a communication failure is generated or not (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected, paragraph 0073, paragraph 0074), a communication failure alerting unit which alerts said management server, in case that it is judged that a communication failure is generated in said traffic measuring and judging unit (Chirashnya, paragraph 0047, generates alarm, paragraph 0048, alarms are sent to primary node), and a traffic log recording unit which records, as a traffic log, communication information of a communication packet judged not to be the communication packet with said format in said first filter and a communication packet judged not to be the communication packet transmitted from said host computer

permitted to access in the second filter (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected), and said management server comprises a display device which displays the alert received from said communication failure alerting unit (Chirashnya, paragraph 0069, receive alarms and generate recommendations, paragraph 0059, user interface), and referring to traffic logs to determine the source of failures (Chirashnya, paragraphs 0047-0048, event collection of packet corruption, paragraph 0059, look for greater failure rate than expected). Chirashnya fails to teach a second filter, traffic log for communications relating to the second filter, or an improper communication source-analyzing unit. However, Yoshida teaches a second filter which receives the communication packet judged to be for said access in said first filter, and judges whether it is a communication packet permitted to access to a storage area in said storage subsystem and transmitted from said host computer or not (Yoshida, column 4 lines 6-26, determines if permission to access network storage device should be granted) and an improper communication source analyzing unit that is alerted from a communication failure alerting unit of said storage subsystem that a communication failure is generated (Yoshida, column 9 lines 55-67, table 1, log the denied storage request), and a traffic log of communication failures of the second filter (Yoshida, column 9 lines 55-67, table 1, log the denied storage request). In addition, Gleichauf teaches a relay device control unit which controls, based on information of a source searched in said improper communication source analyzing unit, a relay device which relays communication to said storage subsystem disposed on said communication line so as to cut off communication from the source (Gleichauf, column 8 lines 18-27, records numbers of attempts to break firewall, column 9 lines 1-30, pattern or data matching, column 13 lines 15-20, communication may be disabled). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Yoshida's method of determining access rights and Gleichauf's security system with Chriashnya's network diagnostic system because it offers the advantage of improving the security of network storage devices by preventing impersonation attacks (Yoshida, column 2 lines 4-10 and column 6 lines 1-26) and allowing the isolation of an invective or attacking network element thus reducing the danger of loss of data or system integrity (Gleichauf, column 1 lines 40-55, column 2 lines 45-60).

16. **With regards to claim 16,** Chirashnya as modified teaches that said host computer is permitted to access to said storage subsystem, said interface further comprises an access permission table having information which uniquely specifies the host computer (Yoshida, column 5 lines 1-20, client access permissions, column 6 lines 25-35, access control list), and information which specifies a storage area in said storage subsystem to which the host computer is permitted to access, and said second filter judges whether a communication packet judged to be for use in said access, is transmitted from the host computer permitted to access or not, in accordance with information stored in said access permission table (Yoshida, column 5 lines 10-25, validates requests on a per packet basis in view of the client access permissions).

17. **With regards to claim 17,** Chirashnya teaches said traffic measuring and judging unit further measures traffic of a communication packet judged not to be the

communication packet transmitted from said host computer permitted to access in said second filter, and by using the traffic and said traffic of all communication packets, further judges whether a communication failure is generated or not (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected).

18. **With regards to claim 18,** Chirashnya teaches said traffic measuring and judging unit further measures traffic of a communication packet judged to be the communication packet transmitted from said host computer permitted to access in said second filter (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected, Yoshida, column 5 lines 1-20, client access permissions, column 6 lines 25-35, access control list), and by using the traffic and said traffic of all communication packets, judges whether a value of a ratio of traffic of a communication packet transmitted from said host computer permitted to access to traffic of all communication packets is less than a predetermined value or not (Chirashnya, paragraph 0047, monitors look for packet corruption, paragraph 0059, look for greater failure rate than expected, Yoshida, column 5 lines 1-20, client access permissions, column 6 lines 25-35, access control list), and said communication failure alerting unit alerts said management server of the alert which indicates that second communication failure is generated (Chirashnya, paragraph 0069, receive alarms and generate recommendations, paragraph 0059, user interface), in case that it is judged that the value of the ratio is less than the predetermined value in the traffic measuring and judging unit, and said management server further comprises a QoS condition

designating unit which, in case of having received the alert which indicates that the second communication failure is generated from said communication failure alerting unit, readjusts a network QoS between said storage subsystem and said host computer, which has been set up in advance by an administrator (Chirashnya, paragraph 0063-0064, determines fault condition and automatically invokes procedure to determine if fault exists, Gleichauf, column 13 lines 15-20, communication may be disabled).

19. **Claim 21 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Chirashnya et al US PGPub 2002/0019870 in view of Blightman et al US Patent No. 7,185,266.

20. **With regards to claim 21,** Chirashnya fails to teach a header of the communication packet with the predetermined format includes information which shows that an iSCSI command is encapsulated in the communication packet. However, Blightman teaches a header of the communication packet with the predetermined format includes information which shows that an iSCSI command is encapsulated in the communication packet (Blightman, column 14 lines 55-65, iSCSI header). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Blightman's iSCSI method because it offers the advantage of providing a standard network storage protocol that allows for detecting of errors (Blightman, column 2 lines 54-67, column 1 lines 35-50).

21. **Claim 22 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Chirashnya et al US PGPub 2002/0019870, Yoshida et al US Patent No. 6,622,220, and Gleichauf US Patent No. 7,137,145, as applied to claim 18 above, and in further view of Blightman et al US Patent No. 7,185,266.

22. **With regards to claim 22,** Chirashnya as modified fails to teach a header of the communication packet with the predetermined format includes information which shows that an iSCSI command is encapsulated in the communication packet. However, Blightman teaches a header of the communication packet with the predetermined format includes information which shows that an iSCSI command is encapsulated in the communication packet (Blightman, column 14 lines 55-65, iSCSI header). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Blightman's iSCSI method because it offers the advantage of providing a standard network storage protocol that allows for detecting of errors (Blightman, column 2 lines 54-67, column 1 lines 35-50).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW L. NALVEN whose telephone number is (571)272-3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Andrew L Nalven/
Examiner, Art Unit 2134

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134